IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF NEW YORK

In re Practice Resources, LLC Data Security Breach Litigation	**Case No. 22-CV-0890** **JURY TRIAL DEMANDED**

MASTER CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs James Stewart ("Mr. Stewart"), Susan Stewart ("Mrs. Stewart"), John Bachura ("Mr. Bachura"), Steven N. Esce ("Mr. Esce"), Brenda Sparks ("Ms. Sparks"), and Gloria Hamilton ("Ms. Hamilton") (collectively, "Plaintiffs"), on behalf of themselves and all others similarly situated, by and through undersigned counsel, hereby allege the following against Practice Resources, LLC ("Defendant" or "PRL"). Facts pertaining to Plaintiffs and their personal experiences and circumstances are alleged based upon personal knowledge, and all other facts herein are alleged based upon information and belief, as well as, *inter alia*, the investigation of Plaintiffs' counsel.

NATURE OF THE CASE

1. This is a class action lawsuit for damages against PRL for its failure to exercise reasonable care in securing and safeguarding patients' and employees' sensitive personal data—including names, home addresses, dates of birth, dates of treatment, health plan numbers, medical record numbers, and Social Security numbers.

2. This class action lawsuit is brought on behalf of individuals whose sensitive personally identifiable information ("PII") and non-public personal health information ("PHI")[1]

[1] This information is collectively referred to as "PII and PHI" or collectively, "Private Information."

was stolen by cybercriminals in a cyber-attack on PRL's systems that took place in or around April 12, 2022, and which resulted in the access and exfiltration of sensitive patient and employee information (the "Data Breach").

3. Defendant discovered the first signs of the Data Breach on or around April 12, 2022, and concluded——through its internal investigation of the Data Breach—that Plaintiffs' and Class members' Private Information was accessed on or about June 5, 2022.

4. Defendant did not began notifying affected individuals until at least August 4, 2022.

5. As a result of the Data Breach and Defendant's failure to promptly notify Plaintiffs and Class members of the Data Breach, Plaintiffs and Class members have experienced and will experience various types of misuse of their Private Information in the coming months and years including, but not limited to, unauthorized credit card charges, unauthorized access to email accounts, identity theft, and other fraudulent use of their Private Information.

6. There has been no assurance offered from PRL that all personal data or copies of data have been recovered or destroyed.

7. Accordingly, Plaintiffs, on behalf of themselves and a class of all others similarly situated, assert claims for negligence, negligence per se, breach of third-party beneficiary contract, breach of implied contract, breach of fiduciary duty, declaratory and injunctive relief, and state consumer protection claims.

JURISDICTION AND VENUE

8. PRL's administrative offices are located at 1001 West Fayette Street, Suite 400 in Syracuse, New York 53029.

9. The Court has jurisdiction over Plaintiffs' claims under 28 U.S.C. § 1332(d)(2) ("CAFA"), because (a) there are 100 or more class members, (b) at least one Class member is a

citizen of a state that is diverse from Defendant's citizenship, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

10. The Court has personal jurisdiction because Defendant's principal place of business is located in this District.

11. Venue is proper in this District under 28 U.S.C. § 1391(b)(1) because Defendant maintains its principal place of business in this District and therefore resides in this District pursuant to 28 U.S.C. § 1391(c)(2). A substantial part of the events or omissions giving rise to the Class's claims also occurred in this District.

12. Venue is proper in this District under 28 U.S.C. § 1391(b)(1) because Defendant maintains its principal place of business in this District and therefore resides in this District pursuant to 28 U.S.C. § 1391(c)(2). A substantial part of the events or omissions giving rise to the Class's claims also occurred in this District.

PARTIES

A. Plaintiff James Stewart

13. Plaintiff James Stewart is a resident and citizen of New Hartford, New York, and brings this action in his individual capacity and on behalf of all others similarly situated. Mr. Stewart receives healthcare services through his insurance policy that is funded by the IBEW Local 43 labor union and regularly visits his doctor's office near the New Hartford area. To receive services, Mr. Stewart was required to disclose his Private Information, which was then entered into PRL's database and maintained without his knowledge. In maintaining his Private Information, Defendant expressly and impliedly promised to safeguard Mr. Stewart's Private Information. Defendant, however, did not take proper care of Mr. Stewart's Private Information, leading to its

exposure to, and exfiltration by cybercriminals as a direct result of Defendant's inadequate security measures.

14. On or around August 24, 2022, Mr. Stewart received a notification letter from Defendant stating that his Private Information was compromised by cybercriminals.

15. Mr. Stewart and Class members have faced and will continue to face a certainly impending and substantial risk of future harms as a result of Defendant's ineffective data security measures, as further set forth herein. Some of these harms will include fraudulent charges, medical procedures ordered in patients' names without their permission, and targeted advertising without patient consent.

16. Some of these harms may not materialize for years after the Data Breach, rendering Defendant's notice letter woefully inadequate to prevent the fraud that will continue to occur through the misuse of Class members' information.

17. Mr. Stewart greatly values his privacy, especially while receiving medical services, and would not have paid the amount that he did to receive medical services had he known that his healthcare providers' and insurance companies' billing and professional services provider, PRL, would negligently maintain his Private Information as it did.

B. Plaintiff Susan Stewart

18. Plaintiff Susan Stewart is a resident and citizen of New Hartford, New York, and brings this action in her individual capacity and on behalf of all others similarly situated. Mrs. Stewart receives healthcare services through her husband's insurance policy and regularly visits her doctor's office near the New Hartford area. To receive services, Mrs. Stewart was required to disclose her Private Information, which was then entered into PRL's database and maintained without her knowledge. In maintaining her Private Information, Defendant expressly and impliedly

promised to safeguard Mrs. Stewart's Private Information. Defendant, however, did not take proper care of Mrs. Stewart's Private Information, leading to its exposure to, and exfiltration by cybercriminals as a direct result of Defendant's inadequate security measures.

19. On or around August 24, 2022, Mrs. Stewart received a notification letter from Defendant stating that her Private Information was compromised by cybercriminals.

20. Mrs. Stewart and Class members have faced and will continue to face a certainly impending and substantial risk of future harms as a result of Defendant's ineffective data security measures, as further set forth herein. Some of these harms will include fraudulent charges, medical procedures ordered in patients' names without their permission, and targeted advertising without patient consent.

21. Some of these harms may not materialize for years after the Data Breach, rendering Defendant's notice letter woefully inadequate to prevent the fraud that will continue to occur through the misuse of Class members' information.

22. Mrs. Stewart greatly values her privacy, especially while receiving medical services, and would not have paid the amount that she did to receive medical services had she known that her healthcare providers' and insurance companies' billing and professional services provider, PRL, would negligently maintain her Private Information as it did.

C. Plaintiff John Bachura

23. Plaintiff John Bachura is a resident and citizen of Onondaga County, New York, and brings this action in his individual capacity and on behalf of all others similarly situated.

24. Mr. Bachura was a patient at Defendant's customer, Family Care Medical Group, PC, at its West Taft Family Care ("West Taft") location in Liverpool, New York.

25. As a condition of receiving West Taft's products and services, Mr. Bachura disclosed his Private Information to West Taft. He trusted that the information would be safeguarded according to internal policies and state and federal law.

26. Mr. Bachura's Private Information was then maintained by Defendant.

27. At the time of the Data Breach, Defendant retained Plaintiff's name, address, diagnostic information, and health insurance information.

28. In maintaining his Private Information, Defendant expressly and impliedly promised to safeguard Mr. Bachura's Private Information. Defendant, however, did not take proper care of Mr. Bachura's Private Information, leading to its exposure to, and exfiltration by cybercriminals as a direct result of Defendant's inadequate security measures.

29. On or around August 23, 2022, Defendant notified Mr. Bachura that its network had been accessed and Plaintiff's Private Information had been involved in the Data Breach.

30. Mr. Bachura and Class members have faced and will continue to face a certainly impending and substantial risk of future harms as a result of Defendant's ineffective data security measures, as further set forth herein. Some of these harms will include fraudulent charges, medical procedures ordered in patients' names without their permission, and targeted advertising without patient consent.

31. Mr. Bachura is very careful about sharing his sensitive PII and PHI. Plaintiff has never knowingly transmitted unencrypted sensitive PII and PHI over the internet or any other unsecured source. He stores any documents containing his sensitive PII and PHI in a safe and secure location or destroys the documents, and he diligently chooses unique usernames and passwords for his various online accounts. Nevertheless, this Data Breach has, through no fault of his own, exposed him to greater risk.

32. Some of these harms may not materialize for years after the Data Breach, rendering Defendant's notice letter woefully inadequate to prevent the fraud that will continue to occur through the misuse of Class members' information.

33. Mr. Bachura greatly values his privacy, especially while receiving medical services, and would not have paid the amount that he did to receive medical services had he known that his healthcare providers' and insurance companies' billing and professional services provider, PRL, would negligently maintain his Private Information as it did.

D. Plaintiff Steven N. Esce

34. Plaintiff Steven N. Esce is a resident and citizen of Fayetteville, New York, and brings this action in his individual capacity and on behalf of all others similarly situated. Mr. Esce's neurologist is associated with Crouse Medical Practice, PLLC, and his medically-ordered laboratory tests are usually processed by Laboratory Alliance of Central New York, LLC. Both of these entities utilized PRL's professional services. To receive medical care, Mr. Esce was required to disclose his Private Information, which was then entered into PRL's database and maintained without his knowledge.

35. In maintaining his Private Information, Defendant expressly and impliedly promised to safeguard Mr. Esce's Private Information. Defendant, however, did not take proper care of Mr. Esce's Private Information, leading to its exposure to, and exfiltration by cybercriminals as a direct result of Defendant's inadequate security measures.

36. On or around August 24, 2022, Mr. Esce received a notification letter from Defendant stating that his Private Information was compromised by cybercriminals.

37. Mr. Esce and Class members have faced and will continue to face a certainly impending and substantial risk of future harms as a result of Defendant's ineffective data security

measures, as further set forth herein. Some of these harms will include fraudulent charges, medical procedures ordered in patients' names without their permission, and targeted advertising without patient consent.

38. Some of these harms may not materialize for years after the Data Breach, rendering Defendant's notice letter woefully inadequate to prevent the fraud that will continue to occur through the misuse of Class members' information.

39. Mr. Esce greatly values his privacy, especially while receiving medical services, and would not have paid the amount that he did to receive medical services had he known that his healthcare providers' and insurance companies' billing and professional services provider, PRL, would negligently maintain his Private Information as it did.

E. Plaintiff Brenda Sparks

40. Plaintiff Brenda Sparks is a resident and citizen of Cazenovia, New York, and brings this action in her individual capacity and on behalf of all others similarly situated. Ms. Sparks was a patient at Upstate Community Medical, PC. Upstate Community Medical is one of PRL's customers.

41. To receive services, Ms. Sparks was required to disclose her Private Information, which was then entered into PRL's database and maintained without her knowledge. In maintaining her Private Information, Defendant expressly and impliedly promised to safeguard Ms. Sparks's Private Information. Defendant, however, did not take proper care of Ms. Sparks's

Private Information, leading to its exposure to, and exfiltration by cybercriminals as a direct result of Defendant's inadequate security measures.

42. Ms. Sparks received a notification letter from Defendant stating that her Private Information was compromised by cybercriminals.

43. Ms. Sparks and Class members have faced and will continue to face a certainly impending and substantial risk of future harms as a result of Defendant's ineffective data security measures, as further set forth herein. Some of these harms will include fraudulent charges, medical procedures ordered in patients' names without their permission, and targeted advertising without patient consent.

44. Some of these harms may not materialize for years after the Data Breach, rendering Defendant's notice letter woefully inadequate to prevent the fraud that will continue to occur through the misuse of Class members' information.

45. In Ms. Sparks's case, that harm is already here. Cybercriminals used her name and personal identifying information to apply for a credit card on or around September 13, 2022, from Bank of America. Cybercriminals also falsely filed a change-of-address form in her name with the United States Postal Service on or around September 17, 2022, which would have allowed them to receive Ms. Spark's mail had she not disputed the change of address.

46. Ms. Sparks greatly values her privacy, especially while receiving medical services, and would not have paid the amount that she did to receive medical services had she known that her healthcare providers' and insurance companies' billing and professional services provider, PRL, would negligently maintain her Private Information as it did.

F. Plaintiff Gloria Hamilton

47. Plaintiff Gloria Hamilton is a resident and citizen of Cicero, New York, and brings this action in her individual capacity and on behalf of all others similarly situated. Ms. Hamilton has been a patient at Crouse Hospital, one of PRL's customers, and has received medical testing from Laboratory Alliance of Central New York. To receive medical services, Ms. Hamilton was required to disclose her Private Information, which was then entered into PRL's database and maintained without her knowledge. In maintaining her Private Information, Defendant expressly and impliedly promised to safeguard Ms. Hamilton's Private Information. Defendant, however, did not take proper care of Ms. Hamilton's Private Information, leading to its exposure to, and exfiltration by cybercriminals as a direct result of Defendant's inadequate security measures.

48. Ms. Hamilton received a notification letter from Defendant stating that her Private Information was compromised by cybercriminals.

49. Ms. Hamilton and Class members have faced and will continue to face a certainly impending and substantial risk of future harms as a result of Defendant's ineffective data security measures, as further set forth herein. Some of these harms will include fraudulent charges, medical procedures ordered in patients' names without their permission, and targeted advertising without patient consent.

50. Some of these harms may not materialize for years after the Data Breach, rendering Defendant's notice letter woefully inadequate to prevent the fraud that will continue to occur through the misuse of Class members' information.

51. Ms. Hamilton has already suffered hardship as a result of the data breach. On September 6, 2022, she woke up to approximately 4,472 new emails in her inbox, all unsolicited. Later, she discovered that calls to her home phone were being forwarded to an unfamiliar number

in California. Likewise, cybercriminals set up a mail forwarding request with the U.S. Postal Service, sending her mail elsewhere. Using her identity, cybercriminals attempted to take out multiple loans in her name: a car loan and personal loan from Empower Credit Union; a personal loan from Best Egg Personal Loan for approximately $8,500; and another personal loan from SoFi, also for approximately $8,500, that cybercriminals successfully collected.

52. Ms. Hamilton greatly values her privacy, especially while receiving medical services, and would not have paid the amount that she did to receive medical services had she known that her healthcare providers' and insurance companies' billing and professional services provider, PRL, would negligently maintain her Private Information as it did.

G. Defendant

53. Defendant PRL is a New York-based company that provides billing and professional services to health insurance carriers and medical providers. PRL has a principal place of business at 1001 West Fayette Street, Suite 400 in Syracuse, New York. PRL's corporate policies and practices, including those used for data privacy, are established in, and emanate from the State of New York.

FACTS

A. The Data Breach & PRL's Untimely & Deficient Notice.

54. On or about April 12, 2022, Defendant discovered unauthorized activity on its network, which contained patients' Private Information.

55. Defendant determined that Plaintiffs' and Class members' Private Information was accessed on or around June 5, 2022, but it did not provide notice of the breach to the U.S. Department of Health and Human Services (HHS) for nearly two months, not until on or around

August 4, 2022.[2]

56. Several weeks after disclosing the breach to the HHS Portal and other state entities, Defendant publicly announced that it suffered a cyberattack that allowed an unauthorized individual to obtain the Private Information of patients within the company's computer systems.[3]

57. Upon learning of the Data Breach, Defendant investigated and began sending notification of the incident to affected parties.

58. On or about August 23, 2022, Defendant sent form notification letters to Plaintiffs and other affected parties (the "Notice"). The form letter including the following:

> **What Happened**
>
> Practice Resources, LLC ("PRL"), which provides billing and other professional services to a number of healthcare entities, is committed to safeguarding the privacy and security of the information entrusted to it. On April 12, 2022, we were subject to a ransomware attack (the "Incident"). With assistance from third-party experts, we took immediate steps to secure our systems and investigate the nature and scope of the Incident. As part of our extensive investigation, we worked diligently to identify any protected health information ("PHI") and personally identifiable information ("PII") that may have been subject to unauthorized access or acquisition as a result of the Incident. On or about June 5, 2022, we identified the individuals whose PHI and/or PII may have been impacted and are in the process of notifying those individuals. We found no evidence that information was misused as a result of this Incident.
>
> **What Information Was Involved**
>
> The Incident may have resulted in unauthorized access to or acquisition of the following information related to the affected individuals: name, home address, dates of treatment, health plan number, and/or medical record number.

---

[2] *Cases Currently Under Investigation*, U.S. DEP'T OF HEALTH & HUM. SERVS., https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

[3] Practice Resources, LLC, *Notice of Data Incident*, https://www.prldocs.com/notice-of-data-incident/ (last visited August 24, 2022).

> **What We Are Doing**
>
> Out of an abundance of caution, we are providing this notice so that all potentially affected individuals can take steps to minimize the risk that their information will be misused. As an added precaution, we have arranged for Cyberscout (through Identity Force) to provide at least 12 months of free credit monitoring and related services to potentially affected individuals. To find out whether you were among those whose information was potentially affected, please contact 1-866-667-1465, from 8:00 am to 8:00 pm Eastern time, Monday through Friday, excluding holidays.
>
> We treat all sensitive information in a confidential manner and are proactive in the careful handling of such information. Since the Incident, we have implemented a series of cybersecurity enhancements and will soon roll out others.
>
> **What You Can Do**
>
> In addition to enrolling in the free credit monitoring and related services mentioned above, we recommend that you remain vigilant and take the following steps to protect your identity, credit, and personal information . . .

59. Defendant offered no explanation for the delay between the initial discovery of the Data Breach and the belated notification to affected patients, which resulted in Plaintiffs and Class members suffering harm they otherwise could have avoided had a timely disclosure been made.

60. Defendant's Notice of the Data Breach was not just untimely but woefully deficient as it failed to provide basic details, including, but not limited to: how unauthorized parties accessed its networks, whether the information was encrypted or otherwise protected, how it learned of the Data Breach, whether the Breach occurred system-wide, whether servers storing information were accessed, and how many customers were affected by the Data Breach.

61. Nor does the notice provide a clear explanation of the risk Plaintiffs and Class members face as a result of the loss of their Private Information, and it only "recommends" that Class members take advantage of free, publicly available resources to monitor their accounts

62. Moreover, PRL's offer to provide 12 months of credit monitoring is woefully inadequate. Credit monitoring only alerts individuals to the misuse of their information after it happens, which might not take place until years after the Data Breach

63. In light of the types of personal information at issue, and the fact that the Private Information was specifically targeted by cybercriminals with the intent to steal and to misuse it, it can be determined that Plaintiffs' and Class members' PII is being sold on the dark web, meaning that unauthorized parties have accessed, viewed, and exfiltrated Plaintiffs' and Class members' unencrypted, unredacted, sensitive personal information, including names, addresses, dates of treatment, health plan numbers, medical record numbers and more as a result of Defendant's lax data security practices and protocols.

64. The Data Breach occurred because Defendant failed to take reasonable measures to protect the PII it collected and stored. Among other things, Defendant failed to implement data security measures designed to prevent this attack, despite repeated warnings to the healthcare industry, insurance companies, and associated entities about the risk of cyberattacks and the highly publicized occurrence of many similar attacks in the recent past on other healthcare providers.

65. Defendant disregarded the rights of Plaintiffs and Class members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiffs' and Class members' PII was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiffs and Class members was compromised through unauthorized access by an unknown third party.

66. Plaintiffs and Class members have a continuing interest in ensuring that their

information is and remains safe.

B. PRL Failed to Maintain Reasonable and Adequate Security Measures to Safeguard Patient Private Information.

67. PRL acquires, collects, and stores a massive amount of its customers' patients' protected PII, including health information and other personally identifiable data.

68. As a condition of engaging in health-related services, PRL requires that its customers entrust it with their patients' highly confidential Private Information.

69. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class members' Private Information, PRL assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class members' Private Information from disclosure.

70. Defendant had obligations created by the Health Insurance Portability and Accountability Act (42 U.S.C. § 1320d *et seq*.) ("HIPAA"), New York law (including N.Y. Gen. Bus. Law § 899-aa, *et seq.*), data breach reporting requirements, industry standards, common law, and representations made to Class members, to keep Class members' Private Information confidential and to protect it from unauthorized access and disclosure.

71. As evidenced by Defendant's failure to comply with the legal obligations established by HIPAA and New York law, Defendant failed to properly safeguard Class members' Private Information, allowing hackers to access their Private Information.

72. Plaintiffs and Class members provided their Private Information to their medical providers and insurance companies with the reasonable expectation and mutual understanding that Defendant and any of its affiliates would comply with their obligation to keep such information confidential and secure from unauthorized access.

73. Prior to and during the Data Breach, Defendant promised its customers that their patients' Private Information would be kept confidential.

74. Defendant's failure to provide adequate security measures to safeguard patients' Private Information is especially egregious because Defendant operates in a field which has recently been a frequent target of scammers attempting to fraudulently gain access to customers' highly confidential Private Information.

75. In fact, Defendant has been on notice for years that the healthcare industry is a prime target for scammers because of the amount of confidential patient information maintained.

76. Defendant was also on notice that the FBI has been concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[4]

77. The American Medical Association ("AMA") has also warned healthcare companies about the important of protecting their patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only

[4] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, REUTERS (Aug. 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warnshealthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820.

> threaten the privacy and security of patients' health and financial information, but also patient access to care.[5]

78. The number of US data breaches surpassed 1,000 in 2016, a record high and a forty percent increase in the number of data breaches from the previous year.[6] In 2017, a new record high of 1,579 breaches were reported—representing a 44.7 percent increase.[7] That trend continues.

79. The healthcare sector reported the second largest number of breaches among all measured sectors in 2018, with the highest rate of exposure per breach.[8] Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[9] Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the customers were

---

[5] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, AM. MED. ASS'N (Oct. 4, 2019), https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals.

[6] Identity Theft Resource Center, *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout* (Jan. 19, 2017), https://www.idtheftcenter.org/surveys-studys.

[7] Identity Theft Resource Center, *2017 Annual Data Breach Year-End Review*, https://www.idtheftcenter.org/2017-data-breaches/.

[8] Identity Theft Resource Center, *2018 End -of-Year Data Breach Report*, https://www.idtheftcenter.org/2018-data-breaches/.

[9] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for- victims/.

never able to resolve their identity theft at all. Data breaches and resulting identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.[10]

80. A 2017 study conducted by HIMSS Analytics showed that email was the most likely cause of a data breach, with 78 percent of providers stating that they experienced a healthcare ransomware or malware attack in the past 12 months.

81. Healthcare related data breaches continued to rapidly increase into 2020 when PRL was breached.[11]

82. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precaution for protection."[12]

83. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.

- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

---

10 *Id.*

11 *2019 HIMSS Cybersecurity Survey*, https://www.himss.org/2019-himsscybersecurity-survey.

12 *See How to Protect Your Networks from RANSOMWARE*, FBI (2016) https ://www. fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view.

- Configure firewalls to block access to known malicious IP addresses.

- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

- Set anti-virus and anti-malware programs to conduct regular scans automatically.

- Manage the use of privileged accounts based on the principle of least privilege; no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

84. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- **Update and patch your computer.** Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks . . .

- **Use caution with links and when entering website addresses.** Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net) . . .

- **Open email attachments with caution.** Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe.** Check a website's security to ensure the information you submit is encrypted before you provide it . . .

- **Verify email senders.** If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself.** Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques.

> You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.
>
> - **Use and maintain preventative software programs.** Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic . . .[13]

85. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

> - **Secure internet-facing assets**
>   - Apply the latest security updates
>   - Use threat and vulnerability management
>   - Perform regular audit; remove privilege credentials;
>
> - **Thoroughly investigate and remediate alerts**
>   - Prioritize and treat commodity malware infections as potential full compromise
>
> - **Include IT Pros in security discussions**
>   - Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;
>
> - **Build credential hygiene**
>   - use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords
>
> - **Apply principle of least-privilege**
>   - Monitor for adversarial activities
>   - Hunt for brute force attempts

[13] *See Security Tip (ST19-001) Protecting Against Ransomware*, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (Apr. 11, 2019), https://us-cert.cisa.gov/ncas/tips/ST19-001.

- Monitor for cleanup of Event Logs
- Analyze logon events

- **Harden infrastructure**
  - Use Windows Defender Firewall
  - Enable tamper protection
  - Enable cloud-delivered protection
  - Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[14]

86. These are basic, common-sense security measures that every business, not only healthcare businesses, should be doing. PRL, with its heightened standard of care, should be doing even more. By adequately taking these common-sense measures, PRL could have prevented this Data Breach from occurring.

87. Charged with handling sensitive PII including healthcare information, PRL knew, or should have known, the importance of safeguarding its customers' patients' Private Information that was entrusted to it and of the foreseeable consequences if its data security systems were breached. This includes the significant costs that would be imposed on the patients in PRL's database as a result of a breach. PRL failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

88. With respect to training, PRL specifically failed to:

- Implement a variety of anti-ransomware training tools, in combination, such as computer-based training, classroom training, monthly newsletters, posters, login alerts, email alerts, and team-based discussions;
- Perform regular training at defined intervals such as bi-annual training and/or monthly security updates; and

[14] *See Human-operated ransomware attacks: A preventable disaster*, MICROSOFT (Mar. 5, 2020), https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-apreventable-disaster/.

- Craft and tailor different approaches to different employees based on their base knowledge about technology and cybersecurity.

89. The PII was also maintained on PRL's computer system in a condition vulnerable to cyberattacks such as through the infiltration of Defendant's systems through ransomware attacks. The mechanism of the cyberattack and the potential for improper disclosure of Plaintiffs' and Class members' PII was a known risk to PRL, and thus PRL was on notice that failing to take reasonable steps necessary to secure the PII from those risks left the PII in a vulnerable position.

C. The Monetary Value of Privacy Protections and Private Information.

90. The fact that Plaintiffs' and Class members' Private Information was stolen means that their members' information is likely for sale by cybercriminals and will be misused in additional instances in the future.

91. At all relevant times, Defendant was well aware that Private Information it collects from Plaintiffs and Class members is highly sensitive and of significant value to those who would use it for wrongful purposes.

92. Private Information is a valuable commodity to identity thieves. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identify theft, and medical and financial fraud.[15] Indeed, a robust "cyber black market" exists in which criminals openly post stolen PII including sensitive health information on multiple underground Internet websites, commonly referred to as the dark web.

93. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information:

[15] Federal Trade Commission, *Warning Signs of Identity Theft* (Sept. 2018), https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft.

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[16]

94. Commissioner Swindle's 2001 remarks are even more relevant today, as consumers' personal data functions as a "new form of currency" that supports a $26 Billion per year online advertising industry in the United States.[17]

95. The FTC has also recognized that consumer data is a new (and valuable) form of currency. In an FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis—and profit.[18]

96. Recognizing the high value that consumers place on their Private Information, many companies now offer consumers an opportunity to sell this information.[19] The idea is to

---

16 *Public Workshop: The Information Marketplace: Merging and Exchanging Consumer Data*, FED. TRADE COMM'N Tr. at 8:2-8 (Mar. 13, 2001), https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf.

17 *See* Julia Angwin & Emily Steel, *Web's Hot New Commodity: Privacy*, The Wall Street Journal (Feb. 28, 2011), http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html [hereinafter *Web's New Hot Commodity*].

18 *Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable*, FED. TRADE COMM'N (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf.

19 *Web's Hot New Commodity*, *supra* note 8.

give consumers more power and control over the type of information that they share and who ultimately receives that information. And, by making the transaction transparent, consumers will make a profit from their Private Information. This business has created a new market for the sale and purchase of this valuable data.

97. Consumers place a high value not only on their Private Information, but also on the privacy of that data. Researchers have begun to shed light on how much consumers value their data privacy, and the amount is considerable. Indeed, studies confirm that the average direct financial loss for victims of identity theft in 2014 was $1,349.[20]

98. The value of Plaintiffs' and Class members' Private Information on the black market is substantial. Sensitive health information can sell for as much as $363.[21] This information is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

99. Medical identity theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial

---

[20] *See* U.S. Dep't of Justice, *Victims of Identity Theft*, OFFICE OF JUSTICE PROGRAMS: BUREAU OF JUSTICE STATISTICS 1 (Nov. 13, 2017), https://www.bjs.gov/content/pub/pdf/vit14.pdf [hereinafter *Victims of Identity Theft*].

[21] Center for Internet Security, *Data Breaches: In the Healthcare Sector*, https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/.

repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[22]

100. The ramifications of PRL's failure to keep its customers' patients' Private Information secure are long-lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for 6 to 12 months or even longer.

101. Approximately 21% of victims do not realize their identity has been compromised until more than two years after it has happened.[23] This gives thieves ample time to seek multiple treatments under the victim's name. Forty percent of consumers found out they were a victim of medical identity theft only when they received collection letters from creditors for expenses that were incurred in their names.[24]

102. Breaches are particularly serious in healthcare industries. The healthcare sector reported the second largest number of breaches among all measured sectors in 2018, with the highest rate of exposure per breach.[25] Indeed, when compromised, healthcare related data is among the most private and personally consequential. A report focusing on healthcare breaches found that

---

[22] Michael Ollove, *The Rise of Medical Identity Theft in Healthcare*, KAISER (Feb. 7, 2014) https://khn.org/news/rise-of-indentity-theft/.

[23] *See Medical ID Theft Checklist*, IDENTITYFORCE, https://www.identityforce.com/blog/medical-id-theft-checklist-2.

[24] *The Potential Damages and Consequences of Medical Identify Theft and Healthcare Data Breaches*, EXPERIAN, (Apr. 2010), https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf.

[25] Identity Theft Resource Center, *2018 End-of-Year Data Breach Report*, (2019) https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf.

the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[26] Almost 50% of the surveyed victims lost their healthcare coverage as a result of the incident, while nearly 30% said their insurance premiums went up after the event. Forty percent of the victims were never able to resolve their identity theft at all. Seventy-four percent said that the effort to resolve the crime and restore their identity was significant or very significant. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.[27]

103. At all relevant times, Defendant was well-aware, or reasonably should have been aware, that the Private Information it maintains is highly sensitive and could be used for wrongful purposes by third parties, such as identity theft and fraud. Defendant should have particularly been aware of these risks, given the significant number of data breaches affecting the healthcare industry and related industries.

104. Had Defendant remedied the deficiencies in its security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, Defendant would have prevented the ransomware attack into its systems and, ultimately, the theft of the Private Information of patients within its systems.

105. The compromised Private Information in the Data Breach is of great value to hackers and thieves and can be used in a variety of ways. Information about, or related to, an individual for which there is a possibility of logical association with other information is of great

---

[26] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for- victims/.

[27] *Id.*

value to hackers and thieves. Indeed, "there is significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer or device even if the individual pieces of data do not constitute PII."[28] For example, different PII elements from various sources may be able to be linked in order to identify an individual, or access additional information about or relating to the individual.[29] Based upon information and belief, the unauthorized parties have already utilized, and will continue utilize, the Private Information they obtained through the Data Breach to obtain additional information from Plaintiffs and Class members that can be misused.

106. In addition, as technology advances, computer programs may scan the Internet with wider scope to create a mosaic of information that may be used to link information to an individual in ways that were not previously possible. This is known as the "mosaic effect."

107. Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts. Thus, even if payment card information were not involved in the Data Breach, the unauthorized parties could use Plaintiffs' and Class members' Private Information to access accounts, including, but not limited to email accounts and financial accounts, to engage in the fraudulent activity identified by Plaintiffs.

---

[28] *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, Preliminary FTC Staff Report*, FED. TRADE COMM'N 35-38 (Dec. 2010), https://www.ftc.gov/reports/preliminary-ftc-staff-report-protecting-consumer-privacy-era-rapid-change-proposed-framework.

[29] *See id.* (evaluating privacy framework for entities collecting or using consumer data with can be "reasonably linked to a specific consumer, computer, or other device").

108. Given these facts, any company that transacts business with customers and then compromises the privacy of customers' Private Information has thus deprived customers of the full monetary value of their transaction with the company.

109. Acknowledging the damage to Plaintiffs and Class members, Defendant instructed affected patients like Plaintiffs to "remain vigilant and take the following steps to protect your identity, credit, and personal information." Plaintiffs and the other Class members now face a greater risk of identity theft.

110. In short, the Private Information exposed is of great value to hackers and cyber criminals and the data compromised in the Data Breach can be used in a variety of unlawful manners, including opening new credit and financial accounts in users' names.

D. PRL's Conduct violated HIPAA.

111. HIPAA requires covered entities like PRL protect against reasonably anticipated threats to the security of PHI. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.[30]

112. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling Private Information like the data Defendant left unguarded. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

[30] *What is Considered Protected Health Information Under HIPAA*?, HIPAA JOURNAL, https://www.hipaajournal.com/what-is-considered-protected-health-information-under-hipaa/.

113. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, also required Defendant to provide notice of the Breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."[31]

114. Defendant's Data Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with safeguards mandated by HIPAA regulations. PRL's security failures include, but are not limited to, the following:

- Failing to ensure the confidentiality and integrity of electronic protected health information that Defendant creates, receives, maintains, and transmits in violation of 45 C.F.R. §164.306(a)(1);

- Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. §164.312(a)(1);

- Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. §164.308(a)(1);

- Failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. §164.308(a)(6)(ii);

- Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 C.F.R. §164.306(a)(2);

- Failing to protect against any reasonably anticipated uses or disclosures of electronically protected health information that are not permitted under the privacy rules regarding individually

[31] *Breach Notification Rule*, U.S. DEP'T HEALTH & HUMAN SERVS., https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html.

identifiable health information in violation of 45 C.F.R. §164.306(a)(3);

- Failing to ensure compliance with HIPAA security standard rules by their workforce in violation of 45 C.F.R. §164.306(a)(94);

- Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 C.F.R. §164.502, *et seq.*;

- Failing to effectively train all members of their workforce (including independent contractors) on the policies and procedures with respect to protected health information as necessary and appropriate for the members of their workforce to carry out their functions and to maintain security of protected health information in violation of 45 C.F.R. §164.530(b) and 45 C.F.R. §164.308(a)(5); and

- Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard protected health information, in compliance with 45 C.F.R. §164.530(c).

E. PRL Failed to Comply with FTC Guidelines.

115. PRL was also prohibited by the Federal Trade Commission Act ("FTC Act") (15 U.S.C. §45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799

F.3d 236 (3d Cir. 2015).

116. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[32]

117. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses.[33] The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

118. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[34]

119. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and

---

[32] *Start With Security: A Guide for Business*, FED. TRADE. COMM'N (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf [hereinafter *Start with Security*].

[33] *Protecting Personal Information: A Guide for Business*, FED. TRADE. COMM'M (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf- 0136_proteting-personal-information.pdf.

[34] *Start with Security*, *supra* note 32.

appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

120. PRL was at all times fully aware of its obligation to protect the Private Information of the patients in its database because of its position as a healthcare data processor. PRL was also aware of the significant repercussions that would result from its failure to do so.

121. As evidenced by Defendant's failure to comply with its legal obligations established by the FTC Act, Defendant failed to properly safeguard Class members' Private Information, allowing hackers to access their Private Information

F. PRL Failed to Comply with Healthcare Industry Standards.

122. HHS's Office for Civil Rights has stated:

> While all organizations need to implement policies, procedures, and technical solutions to make it harder for hackers to gain access to their systems and data, this is especially important in the healthcare industry. Hackers are actively targeting healthcare organizations, as they store large quantities of highly Private and valuable data.[35]

123. HHS highlights several basic cybersecurity safeguards that can be implemented to improve cyber resilience that require a relatively small financial investment yet can have a major impact on an organization's cybersecurity posture including: (a) the proper encryption of Private Information; (b) educating and training healthcare employees on how to protect Private Information; and (c) correcting the configuration of software and network devices.

---

[35] *Cybersecurity Best Practices for Healthcare Organizations*, HIPAA JOURNAL (Nov. 1, 2018), https://www.hipaajournal.com/important-cybersecurity-best-practices-for-healthcare-organizations/.

124. Private cybersecurity firms have also identified the healthcare sector as being particularly vulnerable to cyber-attacks, both because of the value of the Private Information which they maintain and because as an industry they have been slow to adapt and respond to cybersecurity threats.[36] They too have promulgated similar best practices for bolstering cybersecurity and protecting against the unauthorized disclosure of Private Information.

125. Despite the abundance and availability of information regarding cybersecurity best practices for the healthcare industry, PRL chose to ignore them. These best practices were known, or should have been known by PRL, whose failure to heed and properly implement them directly led to the Data Breach and the unlawful exposure of Private Information.

G. Plaintiffs and the Class Members Have Suffered Compensable Damages.

126. Plaintiffs and the Class have been damaged by the compromise of their Private Information in the Data Breach.

127. The ramifications of PRL's failure to keep patients' Private Information secure are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to the victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud.[37]

128. In addition to its obligations under state and federal laws and regulations, Defendant owed a common law duty to Plaintiffs and Class members to protect Private Information entrusted to it, including to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting,

[36] *See, e.g., 10 Best Practices For Healthcare Security*, INFOSEC, https://resources.infosecinstitute.com/topics/healthcare-information-security/#gref.

[37] *2014 LexisNexis True Cost of Fraud Study*, LEXISNEXIS (Aug. 2014), https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf.

and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized parties.

129. Defendant further owed and breached its duty to Plaintiffs and Class members to implement processes and specifications that would detect a breach of its security systems in a timely manner and to timely act upon warnings and alerts, including those generated by its own security systems.

130. As a direct result of Defendant's intentional, willful, reckless, and negligent conduct that resulted in the Data Breach, unauthorized parties were able to access, acquire, view, publicize, and/or otherwise commit the identity theft and misuse of Plaintiffs and Class members' Private Information as detailed above, and Plaintiffs and members of the Class are at a heightened and increased substantial risk of suffering, identity theft and fraud.

131. The risks associated with identity theft are serious. While some identity theft victims can resolve their problems quickly, others spend hundreds to thousands of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or be denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

132. Some of the injuries and risks associated with the loss of personal information have already manifested themselves in Plaintiffs' and Class members' lives. Plaintiffs received a cryptically written notice letter from Defendant stating that their information may have been released, and that they should remain vigilant for fraudulent activity on their accounts, with no other explanation of where this information could have gone, or who might have access to it.

133. Moreover, Plaintiffs and the Class have suffered and continue to face a substantial risk of suffering further out-of-pocket fraud losses such as additional fraudulent charges on online accounts, credit card fraud, applications for benefits made fraudulent in their names, loans opened in their names, medical services billed in their names, and identity theft.

134. Plaintiffs and Class members have, may have, and/or will have incurred out of pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

135. Plaintiffs and Class members did not receive the full benefit of their bargain when paying for medical services. Instead, they received services of a diminished value to those described in their agreements with their respective healthcare and insurance institutions, which themselves entered into agreements with PRL solely for the benefit of Plaintiffs and Class members. Plaintiffs and Class members were damaged in an amount at least equal to the difference in the value between the services they thought they paid for (which would have included adequate data security protection) and the services they actually received.

136. Plaintiffs and Class members would not have obtained services from their medical providers had they known that Defendant failed to properly train its employees, lacked safety controls over its computer network, and did not have proper data security practices to safeguard their Private Information from criminal theft and misuse.

137. Plaintiffs and the Class will continue to spend significant amounts of time to monitor their financial and medical accounts for misuse.

138. The theft of Social Security Numbers is particularly detrimental to victims. The U.S. Social Security Administration ("SSA") warns that "[i]dentity theft is one of the fastest

growing crimes in America."[38] The SSA has stated that "[i]dentity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought."[39] In short, "[s]omeone illegally using your Social Security number and assuming your identity can cause a lot of problems."[40]

139. In fact, a new Social Security number is substantially less effective where "other personal information, such as [the victim's] name and address, remains the same" and for some victims, "a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under your new number may make it more difficult for you to get credit."[41]

140. Identity thieves can use a victim's Private Information to commit any number of frauds, such as obtaining a job, procuring housing, or even giving false information to police during an arrest. In the healthcare industry context, Private Information can be used to submit false insurance claims. For Plaintiffs and Class members, this risk creates unending feelings of fear and annoyance. Private information is especially valuable to identity thieves. Defendant knew or should have known this and strengthened its data systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

---

38 *Identity Theft and Your Social Security Number*, SOCIAL SECURITY ADMIN. (Dec. 2013), http://www.ssa.gov/pubs/EN-05-10064.pdf.

39 *Id.*

40 *Id.*

41 *Id.*

141. As a result of the Data Breach, Plaintiffs and Class members' Private Information has diminished in value.

142. The Private Information belonging to Plaintiffs and Class members is, as its name suggests, private, and was inadequately protected by Defendant. Defendant did not obtain Plaintiffs' or Class members' consent to disclose such Private Information to any other person as required by applicable law and industry standards. Instead, Defendant disclosed information about Plaintiffs and the Class that was of an extremely personal and sensitive nature as a direct result of its inadequate security measures.

143. The Data Breach was a direct and proximate result of Defendant's failure to: (a) properly safeguard and protect Plaintiffs' and Class members' Private Information from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and common law; (b) establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiffs' and Class members' Private Information; and (c) protect against reasonably foreseeable threats to the security or integrity of such information.

144. Defendant had the resources necessary to prevent the Data Breach, but neglected to adequately implement data security measures, despite its obligation to protect customer data.

145. Defendant did not properly train its employees, particularly its information technology department, to timely identify and/or avoid ransomware attacks.

146. Had Defendant remedied the deficiencies in its data security systems and adopted security measures recommended by experts in the field, it would have prevented the intrusions into its systems and, ultimately, the theft of Plaintiffs' and Class members' Private Information.

147. As a direct and proximate result of Defendant's wrongful actions and inactions, Plaintiffs and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives.

148. The U.S. Department of Justice's Bureau of Justice Statistics has found that "among victims who had personal information used for fraudulent purposes, twenty-nine percent spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[42]

149. Defendant has not taken any measures to assist Plaintiffs and Class members other than advising them to do the following:

- remain vigilant for incidents of fraud and identity theft;
- review account statements and monitor credit reports for unauthorized activity;
- obtain a copy of free credit reports;
- contact the FTC and/or the state Attorney General's office;
- enact a security freeze on credit files; and
- create a fraud alert.

None of these recommendations, however, require Defendant to expend any effort to protect Plaintiffs' and Class members' Private Information.

150. Defendant's failure to adequately protect Plaintiffs' and Class members' Private Information has resulted in Plaintiffs and Class members having to undertake these tasks, which require extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of money–while Defendant sits by and does nothing to assist those affected by the

[42] *See* U.S. Dep't of Justice, *Victims of Identity Theft*, OFFICE OF JUSTICE PROGRAMS: BUREAU OF JUSTICE STATISTICS 1 (Nov. 13, 2017), https://www.bjs.gov/content/pub/pdf/vit14.pdf [hereinafter *Victims of Identity Theft*].

incident. Instead, as PRL's Data Breach Notice indicates, it is putting the burden on Plaintiffs and Class members to discover possible fraudulent activity and identity theft.

151. Thus, to mitigate harm, Plaintiffs and Class members are now burdened with indefinite monitoring and vigilance of their accounts to an extent that exceeds the monitoring and vigilance of their accounts previously required before the Data Breach.

152. Plaintiffs and Class members have been damaged in several other ways as well. Plaintiffs and Class members have been exposed to an impending, imminent, and ongoing increased risk of fraud, identity theft, and other misuse of their Private Information.

153. Plaintiffs and Class members must now and indefinitely closely monitor their financial and other accounts to guard against fraud.

154. This is a burdensome and time-consuming task. Plaintiffs and Class members have also been forced to purchase adequate credit reports, credit monitoring and other identity protection services, and have placed credit freezes and fraud alerts on their credit reports, while also spending significant time investigating and disputing fraudulent or suspicious activity on their accounts. Plaintiffs and Class members also suffered a loss of the inherent value of their Private Information.

155. Plaintiffs Stark and Hamilton have already been victims of the fraudulent misuse of their Private Information in the wake of the Data Breach, showing that the harms Plaintiffs and the Class have suffered and continue to suffer, including the increased risk of fraud, identity theft, and other misuse of their Private Information, are hardly theoretical.

156. The Private Information stolen in the Data Breach can be misused on its own or can be combined with personal information from other sources such as publicly available information, social media, etc. to create a package of information capable of being used to commit further

identity theft. Thieves can also use the stolen Private Information to send spear-phishing emails to Class members to trick them into revealing sensitive information.

157. Lulled by a false sense of trust and familiarity from a seemingly valid sender (for example Wells Fargo, Amazon, or a government entity), the individual agrees to provide sensitive information requested in the email, such as login credentials, account numbers, and the like.

158. As a result of Defendant's failures to prevent the Data Breach, Plaintiffs and Class members have suffered, will suffer, and are at increased risk of suffering:

- The compromise, publication, theft and/or unauthorized use of their Private Information;
- Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;
- Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;
- The continued risk to their Private Information, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake appropriate measures to protect the Private Information in its possession;
- Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiffs and Class members; and
- Anxiety and distress resulting fear of misuse of their Private Information.

159. In addition to a remedy for the economic harm, Plaintiffs and Class members maintain an undeniable interest in ensuring that their Private Information remains secure and is not subject to

further misappropriation and theft.

CLASS ACTION ALLEGATIONS

160. Plaintiffs incorporate by reference all other paragraphs of this Complaint as if fully set forth herein.

161. Plaintiffs bring this action individually and on behalf of all other persons similarly situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), 23(b)(3), and/or 23(c)(4)

162. Specifically, Plaintiffs propose the following Nationwide Class, as well as a New York Subclass (collectively, the "Class") definitions:

> **Nationwide Class**
>
> All persons residing in the United States whose Private Information was compromised as a result of the Data Breach discovered on or about April of 2022 and who were sent notice of the Data Breach.
>
> **New York Subclass**
>
> All persons residing in New York whose Private Information was compromised as a result of the Data Breach discovered on or about April of 2022 and who were sent notice of the Data Breach.

Excluded from the Class are Defendant and Defendant's affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded are any judicial officers presiding over this matter and the members of their immediate families and judicial staff.

163. Plaintiffs reserve the right to modify, change, amend, or expand the definitions of the Nationwide Class, as well as the New York Subclass, based upon discovery and further investigation.

164. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

165. **Numerosity—Federal Rule of Civil Procedure 23(a)(1).** The members of the Class are so numerous that joinder of all Class members would be impracticable. On information and belief, the Nationwide Class number in the hundreds of thousands.

166. **Commonality and Predominance—Federal Rule of Civil Procedure 23(a)(2).** Common questions of law and fact exist as to all members of the Class and predominate over questions affecting only individual members of the Class. Such common questions of law or fact include, *inter alia*:

a. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

b. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

c. Whether Defendant properly implemented its purported security measures to protect Plaintiffs' and the Class's Private Information from unauthorized capture, dissemination, and misuse;

d. Whether Defendant took reasonable measures to determine the extent of the Data Breach after it first learned of same;

e. Whether Defendant disclosed Plaintiffs' and the Class's Private Information in violation of the understanding that the Private Information was being disclosed in confidence and should be maintained;

f. Whether Defendant willfully, recklessly, or negligently failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiffs' and the Class's Private Information;

g. Whether Defendant was negligent in failing to properly secure and protect Plaintiffs' and the Class's Private Information;

h. Whether Defendant was unjustly enriched by its actions; and

i. Whether Plaintiffs and the other members of the Class are entitled to damages, injunctive relief, or other equitable relief, and the measure of such damages and relief.

Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs, on behalf of themselves and other members of the Class. Similar or identical common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that predominate in this action.

167. **Typicality—Federal Rule of Civil Procedure 23(a)(3).** Plaintiffs' claims are typical of the claims of the other members of the Class because, among other things, all Class members were similarly injured through Defendant's uniform misconduct described above and were thus all subject to the Data Breach alleged herein. Further, there are no defenses available to Defendant that are unique to Plaintiffs.

168. **Adequacy of Representation—Federal Rule of Civil Procedure 23(a)(4).** Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the Class they seek to represent, they have retained counsel competent and experienced in complex class action litigation, and they will prosecute this action vigorously. The Class's interests will be fairly and adequately protected by Plaintiffs and their counsel.

169. **Injunctive Relief-Federal Rule of Civil Procedure 23(b)(2).** Defendant has acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. Civ. P. 23 (b)(2).

170. **Superiority—Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiffs and the Class are relatively small compared to the burden and expense that would be required to individually litigate their claims

against Defendant, so it would be impracticable for members of the Class to individually seek redress for Defendant's wrongful conduct. Even if members of the Class could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

NEW YORK LAW SHOULD APPLY TO ALL PLAINTIFFS AND CLASS MEMBERS' CLAIMS

171. The State of New York has a significant interest in regulating the conduct of businesses operating within its borders.

172. New York, which seeks to protect the rights and interests of New York and all residents and citizens of the United States against a company headquartered and doing business in New York, has a greater interest in the claims of Plaintiffs and the Class than any other state and is most intimately concerned with the claims and outcome of this litigation.

173. The principal place of business and headquarters of PRL, located at 1001 West Fayette Street, Suite 400 in Syracuse, New York 53029, is the "nerve center" of its business activities—the place where its high-level officers direct, control and coordinate Defendant's activities, including major policy, financial and legal decisions.

174. Defendant's actions and corporate decisions surrounding the allegations made in the Complaint were made from and in New York.

175. Defendant's breaches of duty to Plaintiffs and Class Members emanated from New York.

176. Application of New York law to the Classes with respect to Plaintiffs' and the Classes' claims is neither arbitrary nor fundamentally unfair because choice of law principles, which are applicable to this action, the common law of New York applies to the nationwide common law claims of all Class members.

177. Additionally, given New York's significant interest in regulating the conduct of businesses operating within its borders, and that New York has the most significant relationship to Defendant, as it is headquartered in New York, and its executives and officers are located and

made decisions which have given rise to the allegations and claims asserted herein, there is no conflict in applying New York law to non-resident consumers such as Plaintiffs and the Class.

CAUSES OF ACTION

COUNT I

NEGLIGENCE
(On Behalf of Plaintiffs and the Nationwide Class or, Alternatively, Plaintiffs and the New York Subclass)

178. Plaintiffs fully incorporate by reference all of the above paragraphs, as though they are fully set forth herein.

179. Upon Defendant accepting and storing the Private Information of Plaintiffs and the Class in its computer systems and on its networks, Defendant undertook and owed a duty to Plaintiffs and the Class to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Defendant knew that the Private Information was private and confidential and should be protected.

180. Defendant owed a duty of care not to subject Plaintiffs' and the Class's Private Information to an unreasonable risk of exposure and theft because Plaintiffs and the Class were foreseeable and probable victims of any inadequate security practices.

181. Defendant owed numerous duties to Plaintiffs and the Class, including the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting Private Information in its possession;

b. To protect Private Information using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and

c. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

182. Defendant also breached its duty to Plaintiffs and Class members to adequately protect and safeguard Private Information by disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured Private Information.

183. Furthering its dilatory practices, Defendant failed to provide adequate supervision and oversight of the Private Information with which it was and is entrusted, despite the known risk and foreseeable likelihood of breach and misuse, which permitted a malicious third party to gather Plaintiffs and Class members' Private Information and misuse the Private Information and intentionally disclose it to others without consent.

184. Defendant knew, or should have known, of the risks inherent in collecting and storing Private Information and the importance of adequate security. Defendant knew or should have known about numerous well-publicized data breaches within the manufacturing industry.

185. Defendant knew, or should have known, that its data systems and networks did not adequately safeguard Plaintiffs and Class members' Private Information.

186. Defendant breached its duties to Plaintiffs and Class members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class members' Private Information.

187. Because Defendant knew that a breach of its systems would damage thousands of its customers' patients, including Plaintiffs and Class members, Defendant had a duty to adequately protect its data systems and the Private Information contained thereon.

188. Defendant's duty of care to use reasonable security measures arose because of the special relationship that existed between Defendant and its employees, which is recognized by

statute, regulations, and the common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class members from a data breach.

189. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

190. Defendant also had a duty under HIPAA privacy laws, which were enacted with the objective of protecting the confidentiality of clients' healthcare information and set forth the conditions under which such information can be used, and to whom it can be disclosed. HIPAA privacy laws not only apply to healthcare providers and the organizations they work for, but to any entity that may have access to healthcare information about a patient that—if it were to fall into the wrong hands—could present a risk of harm to the patient's finances or reputation.

191. Defendant's own conduct also created a foreseeable risk of harm to Plaintiffs and Class members and their Private Information. Defendant's misconduct included failing to: (1) secure Plaintiffs' and Class members' Private Information; (2) comply with industry standard security practices; (3) implement adequate system and event monitoring; and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

192. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class members' Private Information, and by failing to provide timely notice of the Data Breach.

193. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class members' Private Information;

b. Failing to adequately monitor the security of Defendant's networks and systems;

c. Allowing unauthorized access to Class members' Private Information; and

d. Failing to timely notify Class members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

194. Through Defendant's acts and omissions described in this Complaint, including its failure to provide adequate security and its failure to protect Plaintiffs' and Class members' Private Information from being foreseeably captured, accessed, disseminated, stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure Plaintiffs' and Class members' Private Information during the time it was within Defendant's possession or control.

195. Defendant's conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to failing to adequately protect the Private Information and failing to provide Plaintiffs and Class members with timely notice that their sensitive Private Information had been compromised.

196. Neither Plaintiffs nor the other Class members contributed to the Data Breach and subsequent misuse of their Private Information as described in this Complaint.

197. As a direct and proximate cause of Defendant's conduct, Plaintiffs and Class members suffered damages as alleged above.

198. Plaintiffs and Class members are also entitled to injunctive relief requiring Defendant to, *inter alia*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide lifetime free credit monitoring to all Class members.

COUNT II

NEGLIGENCE *PER SE*
(On Behalf of Plaintiffs and the Nationwide Class or,
Alternatively, Plaintiffs and the New York Subclass)

199. Plaintiffs fully incorporate by reference all of the above paragraphs, as though they are fully set forth herein.

200. Pursuant to the Federal Trade Commission Act (15 U.S.C. § 45), Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

201. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty.

202. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiffs' and Class members' Private Information and not complying with applicable industry standards, as described in detail herein.

203. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of a data breach including, specifically, the damages that would result to Plaintiff and Class members.

204. Defendant's violation of Section 5 of the FTC Act constitutes negligence per se as Defendant' violation of the FTC Act establishes the duty and breach elements of negligence.

205. Plaintiffs and Class members are within the class of persons that the FTC Act was intended to protect.

206. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses which—as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices—caused the same harm as that suffered by Plaintiffs and Class members.

207. Defendant's failure to comply with applicable laws and regulations constitutes negligence per se.

208. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs and Class members, Plaintiffs and Class members would not have been injured.

209. The injury and harm suffered by Plaintiffs and Class members was the reasonably foreseeable result of Defendant's breach of their duties.

210. Defendant knew or should have known that it was failing to meet its duties and that its breach would cause Plaintiffs and Class members to experience the foreseeable harms associated with the exposure of their Private Information.

211. Accordingly, Plaintiffs and the Class are entitled to damages in an amount to be determined at trial, along with their costs and attorneys' fees incurred in this action, as well as appropriate injunctive relief to protect Plaintiffs and Class members from further harm.

COUNT III

BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(On Behalf of Plaintiffs and the Nationwide Class or, Alternatively, the New York Subclass)

212. Plaintiffs fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

213. PRL entered into a contract to provide services to Plaintiffs' respective medical providers and/or insurance companies.

214. Upon information and belief, this contract is virtually identical to the contracts entered into between PRL and its other medical provider and insurance customers around the country whose patients were also affected by the Data Breach.

215. These contracts were made expressly for the benefit of Plaintiffs and the Class, as it was their confidential medical information that PRL agreed to collect and protect through its services. Thus, the benefit of collection and protection of the Private Information belonging to Plaintiffs and the Class was the direct and primary objective of the contracting parties.

216. PRL knew that if it were to breach these contracts with its customers, the customers' patients, including Plaintiffs and the Class, would be harmed by, among other harms, fraudulent transactions.

217. PRL breached its contracts with the medical providers and/or insurance entities affected by this Data Breach when it failed to use reasonable data security measures that could have prevented the Data Breach.

218. As foreseen, Plaintiffs and the Class were harmed by PRL's failure to use reasonable security measures to store patient information, including but not limited to the risk of harm through the loss of their Private Information.

219. Accordingly, Plaintiffs and the Class are entitled to damages in an amount to be determined at trial, along with their costs and attorneys' fees incurred in this action.

COUNT IV

BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Nationwide Class or, Alternatively, the New York Subclass)

220. Plaintiffs fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

221. Plaintiffs bring this claim for breach of implied contract in the alternative to their breach of third-party beneficiary contract claim.

222. Through its course of conduct, Defendant, Plaintiffs, and Class members entered into implied contracts for the provision of healthcare data administration services, as well as implied contracts for the Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiffs' and Class members' Private Information.

223. Specifically, Plaintiffs entered into a valid and enforceable implied contract with Defendant when they first entered into the medical services contract with Defendant.

224. The valid and enforceable implied contracts to provide medical billing and professional services that Plaintiffs and Class members entered into with Defendant include Defendant's promise to protect nonpublic Private Information given to or created by Defendant from disclosure.

225. When Plaintiffs and Class members provided their Private Information to Defendant in exchange for Defendant's services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

226. Defendant solicited and invited Class members to provide their Private Information as part of Defendant's regular business practices. Plaintiffs and Class members accepted Defendant's offers and provided their Private Information to Defendant.

227. In entering into such implied contracts, Plaintiffs and Class members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

228. Plaintiffs and Class members who paid money to Defendant's healthcare customers reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. Part of the of price that they paid was intended to be used to fund adequate data security. Defendant failed to do so.

229. Under implied contracts, Defendant and/or its affiliated providers promised and were obligated to: (a) provide secure medical billing and professional services to Plaintiffs' and Class members' healthcare providers and insurance companies; and (b) protect Plaintiffs and Class members' Private Information provided to obtain the benefits of such services. In exchange, Plaintiffs and Class members agreed to pay money for these services, and to turn over their Private Information.

230. Both the provision of medical services and the protection of Plaintiffs and Class members' Private Information were material aspects of these implied contracts.

231. The implied contracts for the provision of medical service contracts that include the contractual obligations to maintain the privacy of Plaintiffs' and Class members' Private Information are also acknowledged, memorialized, and embodied in multiple documents, including (among other documents) Defendant's Data Breach notification letter and Defendant's relevant privacy policy documents.

232. Defendant's express representations, including, but not limited to the express representations found in its privacy policy, memorializes and embodies the implied contractual

obligation requiring Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiffs' and Class members' Private Information.

233. Consumers of medical services value their privacy, the privacy of their dependents, and the ability to keep confidential their Private Information associated with obtaining such services. Plaintiffs and Class members would not have entrusted their Private Information to Defendant and entered into these implied contracts with Defendant without an understanding that their Private Information would be safeguarded and protected, nor would they have entrusted their Private Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

234. A meeting of the minds occurred, as Plaintiffs and Class members agreed and provided their Private Information to Defendant and/or its affiliated healthcare providers and paid for the provided medical guidance services in exchange for, among other things, both the provision of healthcare and the protection of their Private Information.

235. Plaintiffs and Class members performed their obligations under the contract when they paid for Defendant's services and provided their Private Information.

236. Defendant materially breached its contractual obligation to protect the nonpublic Private Information Defendant gathered when the information was accessed and exfiltrated by the Data Breach.

237. Defendant materially breached the terms of the implied contracts, including, but not limited to, the terms stated in the relevant privacy policy. Defendant did not maintain the privacy of Plaintiffs and Class members' Private Information as evidenced by its notifications of the Data Breach to Plaintiffs and Class members. Specifically, Defendant did not comply with

industry standards, standards of conduct embodied in statutes like Section 5 of the FTCA, or otherwise protect Plaintiffs' and Class members' private information as set forth above.

238. The Data Breach was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.

239. As a result of Defendant's failure to fulfill the data security protections promised in these contracts, Plaintiffs and Class members did not receive full benefit of the bargain, and instead received healthcare and other services that were of a diminished value to that described in the contracts. Plaintiffs and Class members, therefore, were damaged in an amount at least equal to the difference in the value between the healthcare with data security protection they paid for and the healthcare they received.

240. Had Defendant disclosed that its security was inadequate or that it did not adhere to industry-standard security measures, neither Plaintiffs, Class members, nor any reasonable person would have purchased healthcare services from Defendant's affiliated providers, from which services Defendant directly benefits.

241. As a direct and proximate result of the Data Breach, Plaintiffs and Class members will suffer actual damages and injuries, including without limitation the release and disclosure of their Private Information, the loss of control of their Private Information, the imminent risk of suffering additional damages in the future, disruption of their medical care and treatment, out of pocket expenses, and the loss of the benefit of the bargain they had struck with Defendant.

242. Plaintiffs and Class members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

243. Plaintiffs and Class members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit

to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class members.

COUNT V

BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiffs and the Nationwide Class or, Alternatively, the New York Subclass)

244. Plaintiffs fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

245. In providing their Private Information to Defendant, Plaintiffs and Class members justifiably placed a special confidence in Defendant to act in good faith and with due regard for the interests of Plaintiffs and Class members to safeguard and keep confidential that Private Information.

246. Defendant accepted the special confidence Plaintiffs and Class members placed in it, as evidenced by its assertion that it is committed to protecting the privacy of Plaintiffs' personal information as included in the Data Breach notification letter.

247. In light of the special relationship between Defendant, Plaintiffs, and Class members, whereby Defendant became a guardian of Plaintiffs and Class members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for the benefit of its customers, including Plaintiffs and Class members for the safeguarding of Plaintiffs and Class members' Private Information.

248. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class members upon matters within the scope of its customer relationships, in particular, to keep secure the Private Information of its customers.

249. Defendant breached its fiduciary duties to Plaintiffs and Class members by failing to protect the integrity of the systems containing Plaintiffs' and Class members' Private Information.

250. Defendant breached its fiduciary duties to Plaintiffs and Class members by otherwise failing to safeguard Plaintiffs and Class members' Private Information.

251. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class members have suffered and will suffer injury, including but not limited to:

a. Actual identity theft;

b. The compromise, publication, and/or theft of their Private Information;

c. Out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information;

d. Lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft;

e. The continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession;

f. Future costs in terms of time, effort, and money that will be expended as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and

g. The diminished value of the services they paid for and received.

252. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class members will suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT VI

UNJUST ENRICHMENT/ QUASI CONTRACT
(On Behalf of Plaintiffs and the Nationwide Class or, Alternatively, the New York Subclass)

253. Plaintiffs fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

254. Plaintiffs and Class Members conferred a monetary benefit on Defendant. Specifically, they provided Defendant with their Private Information.

255. In exchange, Plaintiffs and Class members should have received from Defendant data storage that was compliant with and maintained in accordance with Defendant's pre-existing duties to secure such information under federal law and industry standards and were entitled to have Defendant protect their Private Information with adequate security.

256. Defendant knew that Plaintiff and Class members conferred a benefit on them and accepted or retained that benefit. Defendant profited from Plaintiffs' and Class Members' Private Information for business purposes.

257. Defendant failed to secure Plaintiffs' and Class members' Private Information and therefore, did not provide full compensation for the benefit the Plaintiffs' and Class members' Private Information provided.

258. Defendant acquired the Private Information through inequitable means as they failed to disclose the inadequate security practices previously alleged.

259. If Plaintiffs and Class Members had known that Defendant would not secure their Private Information using adequate security, they would not have provided their information to Defendant's customers.

260. Plaintiffs and Class Members have no adequate remedy at law.

261. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiffs and Class members conferred on them.

262. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and the Class members overpaid for the use of Defendant's services.

COUNT VII

VIOLATIONS OF NEW YORK'S INFORMATION SECURITY BREACH AND NOTIFICATION ACT (N.Y. Gen. Bus. Law § 899-aa, *et seq.*)
(On Behalf of Plaintiffs and the New York Subclass)

263. Plaintiffs fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

264. The acts and practices alleged herein occurred in trade or commerce in the state of New York.

265. The Data Breach, which compromised the Private Information of New York citizens, constitutes a "breach of security," as that term is defined by NY Gen. Stat. §899-aa.

266. In the manner described herein, Defendant unreasonably delayed the disclosure of the "breach of security" of Private Information within the meaning of NY Gen. Stat. § 899-aa.

267. Pursuant to NT Gen. Stat. § 899-aa the Defendant's failure to disclose the Data Breach following discovery to each New York resident whose Private Information was, or was

reasonably believed to have been, accessed by an unauthorized person through the Breach constitutes an unfair trade practice pursuant to NY. Gen. Stat. § 899-aa.

COUNT VIII

VIOLATIONS OF NEW YORK GENERAL BUSINESS LAW § 349
(N.Y. Gen. Bus. Law § 349 *et seq.* (2019))
(On Behalf of Plaintiffs and the New York Subclass)

268. Plaintiffs fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

269. New York General Business Law ("NYGBL") § 349 prohibits deceptive acts or practices in the conduct of any business, trade, or commerce, or in the furnishing of any service in the state of New York.

270. By reason of the conduct alleged herein, Defendant engaged in unlawful practices within the meaning of the NYGBL § 349. The conduct alleged herein is a "business practice" within the meaning of the NYGBL § 349, and the deception occurred within New York State.

271. Defendant stored Plaintiffs' and Class members' Private Information in Defendant's electronic databases. Defendant knew or should have known it did not employ reasonable, industry standard, and appropriate security measures that complied with all relevant regulations and would have kept Plaintiffs' and Class members' Private Information secure and prevented the loss or misuse of that Private Information. Defendant did not disclose to Plaintiffs and Class members that its data systems were not secure.

272. Plaintiffs and Class members would not have provided their Private Information if they had been told or knew that Defendant failed to maintain sufficient security thereof, and its inability to safely store Plaintiffs' and Class members' Private Information.

273. As alleged herein in this Complaint, Defendant engaged in the unfair or deceptive acts or practices in the conduct of consumer transactions in violation of N.Y. Gen. Bus. Law § 349, including but not limited to:

- Representing that its services were of a particular standard or quality that it knew or should have known were of another;
- Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Class members' Private Information, which was a direct and proximate cause of the Data Breach;
- Failing to identify foreseeable security and privacy risks, and remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;
- Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class members' Private Information, including duties imposed by the FTCA, 15 U.S.C. § 45, which was a direct and proximate cause of the Cyber-Attack and Data Breach;
- Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Class members' Private Information, including by implementing and maintaining reasonable security measures;
- Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Class members' Private Information; and
- Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class members' Personal Information, including duties imposed by the FTCA, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach.

274. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' Private Information.

275. Such acts by Defendant are and were deceptive acts or practices which are and/or were likely to mislead a reasonable consumer providing his or her Private Information to Defendant. Said deceptive acts and practices are material. The requests for and use of such Private Information in New York through deceptive means occurring in New York were consumer-oriented acts and thereby falls under the New York consumer fraud statute, NYGBL § 349.

276. In addition, Defendant's failure to secure patients' Private Information violated the FTCA and therefore violates N.Y. Gen. Bus. Law § 349.

277. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard the PII of Plaintiffs and Class members, deter hackers, and detect a breach within a reasonable time, and that the risk of a data breach was highly likely. Plaintiffs and Class members accordingly seek all monetary and non-monetary relief allowed by law, including actual damages, treble damages, injunctive relief, civil penalties, and attorneys' fees and costs.

278. The aforesaid conduct violated N.Y. Gen. Bus. Law § 349, in that it is a restraint on trade or commerce.

279. Defendant's violations of N.Y. Gen. Bus. Law § 349 have an impact and general importance to the public, including the people of New York. Thousands of New Yorkers have had their Private Information stored on PRL's electronic database, many of whom have been impacted by the Data Breach.

280. In addition, New York residents have a strong interest in regulating the conduct of its retirement and investment services administrators, whose polices described herein have affected thousands of people across the country.

281. As a direct and proximate result of these deceptive trade practices, Plaintiffs and Class members are entitled to judgment under N.Y. Gen. Bus. Law § 349, to enjoin further violations, to recover actual damages, to recover the costs of this action (including reasonable attorneys' fees), and such other relief as the Court deems just and proper.

282. On information and belief, PRL formulated and conceived of the systems used to compile and maintain patient information largely within the state of New York, oversaw its data privacy program complained of herein from New York, and its communications and other efforts to hold participant data largely emanated from New York.

283. Most, if not all, of the alleged misrepresentations and omissions by PRL that led to inadequate measures to protect patient information occurred within or were approved within New York.

284. Defendant's implied and express representations that it would adequately safeguard Plaintiffs' and Class members' Private Information constitute representations as to the particular standard, quality, or grade of services that such services did not actually have (as the services were of another, inferior quality), in violation of N.Y. Gen. Bus. Law § 349.

285. Accordingly, Plaintiffs, on behalf of themselves and Class members, bring this action under N.Y. Gen. Bus. Law § 349 to seek such injunctive relief necessary to enjoin further violations and recover costs of this action, including reasonable attorneys' fees and other costs.

COUNT IX

DECLARATORY RELIEF
(On Behalf of Plaintiffs and the Nationwide Class or,
Alternatively, the New York subclass)

286. Plaintiffs fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

287. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and granting further necessary relief.

288. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal statutes described in this Complaint.

289. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's present and prospective common law and other duties to reasonably safeguard Plaintiffs' and Class members' PII, and whether Defendant is currently maintaining data security measures adequate to protect Plaintiffs and Class members from future data breaches that compromise their Private Information. Plaintiffs and the Class remain at imminent risk that further compromises of their PII will occur in the future.

290. The Court should also issue prospective injunctive relief requiring Defendant to employ adequate security practices consistent with law and industry standards to protect consumers' PII.

291. Defendant still possesses the PII of Plaintiffs and the Class.

292. To Plaintiffs' knowledge, Defendant has made no announcement that it has changed its data storage or security practices relating to the PII.

293. To Plaintiffs' knowledge, Defendant has made no announcement or notification that it has remedied the vulnerabilities and negligent data security practices that led to the Data Breach.

294. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach at PRL. The risk of another such breach is real, immediate, and substantial.

295. The hardship to Plaintiffs and Class members if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Among other things, if another data breach occurs at PRL, Plaintiffs and Class members will likely continue to be subjected to fraud, identify theft, and other harms described herein. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

296. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at PRL, thus eliminating the additional injuries that would result to Plaintiffs and Class members, along with other consumers whose PII would be further compromised.

297. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that PRL implement and maintain reasonable security measures, including but not limited to the following:

a. Engaging third-party security auditors/penetration testers, as well as internal security personnel, to conduct testing that includes simulated attacks, penetration tests, and audits on PRL's systems on a periodic basis, and ordering PRL to

promptly correct any problems or issues detected by such third-party security auditors;

b. Engaging third-party security auditors and internal personnel to run automated security monitoring;

c. Auditing, testing, and training its security personnel regarding any new or modified procedures;

d. Purging, deleting, and destroying Private Information not necessary for its provisions of services in a reasonably secure manner;

e. Conducting regular database scans and security checks; and

f. Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs James Stewart, Susan Stewart, John Bachura, Steven N. Esce, Brenda Sparks, and Gloria Hamilton, individually and on behalf of the other members of the Class proposed in this Complaint, respectfully demand a jury trial of all issues so triable and request that the Court enter judgment in their favor and against Defendant, as follows:

a. Declaring that this action is a proper class action, certifying the Classes as requested herein, designating Plaintiffs as Class Representatives, and appointing Class Counsel as requested in Plaintiffs' expected motion for class certification;

b. Ordering Defendant to pay punitive damages, as allowable by law, to Plaintiffs and the other members of the Class;

c. Ordering injunctive relief requiring Defendant to, *inter alia*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring

procedures; and (iii) immediately provide free credit monitoring to all Class members indefinitely;

d. Ordering Defendant to pay attorneys' fees and litigation costs to Plaintiffs and their counsel;

e. Ordering Defendant to pay equitable relief, in the form of disgorgement and restitution, and injunctive relief as may be appropriate;

f. Ordering Defendant to pay both pre- and post-judgment interest on any amounts awarded; and

g. Ordering such other and further relief as may be just and proper.

JURY DEMAND

Plaintiffs hereby request a trial by jury.

Date: December 22, 2022

Respectfully submitted,

/s/ Nicholas A. Migliaccio
Nicholas A. Migliaccio* (NY Bar # 4035838)
Jason Rathod (pro hac vice forthcoming)
Tyler Bean (pro hac vice forthcoming)
MIGLIACCIO & RATHOD, LLP
412 H Street NE
Washington, D.C. 20002
202.470.3520
nmigliaccio@classlawdc.com

*Permanently admitted in N.D.N.Y.
(Bar Roll Number: 519012)

/s/ James Bilsborrow

James Bilsborrow (Bar Roll #519903)
WEITZ & LUXENBERG, P.C.
700 Broadway
New York, NY 10003
Ph: 212-558-5500
jbilsborrow@weitzlux.com

Counsel for Plaintiffs & the Nationwide Class